OPAM-OIM Integration

How to integrate OPAM to work in tandem with OIM?

Software versions

OPAM - 11g R2 PS2

OIM - 11g R2 PS2

Assumptions: OIM is installed as a part of the Oracle IDAM R2 PS2 suite

Note: OPAM is installed in a separate Weblogic domain than that of OIM

Why integrate OIM and OPAM?

OPAM-OIM integration is primarily done so that ***the access to privilege accounts*** via OPAM can be ***regulated through OIM***.

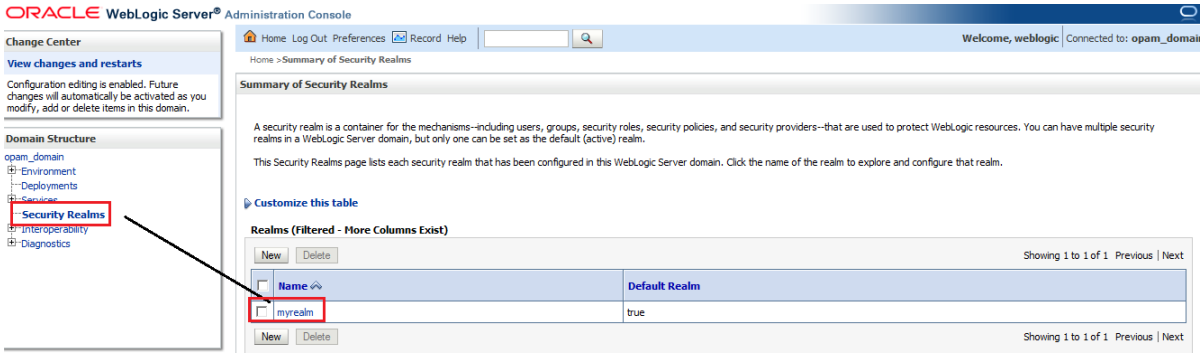
OIM can be ***integrated with the LDAP Identity Store using LDAP Connector or LDAPSync*** and end users can be subjected to an ***request based approval workflow*** in order to get access to certain ***LDAP groups*** in the OPAM Identity Store. These ***LDAP groups in turn can be configured within OPAM*** for managing secure access to Privileged accounts and targets.

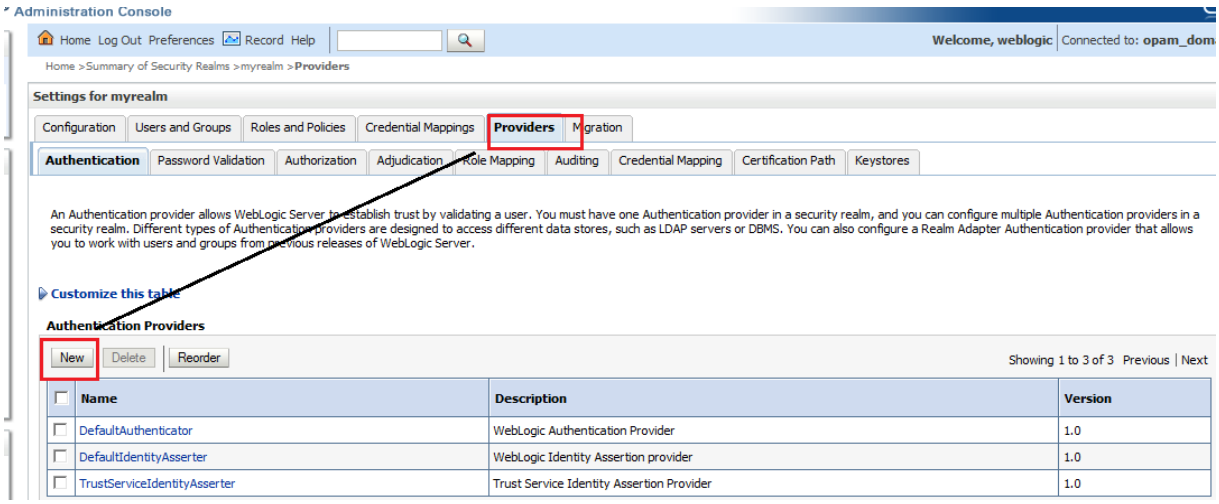
1. Configure the Identity Store for OPAM

   We are going to use Apache DS LDAP server as an example.

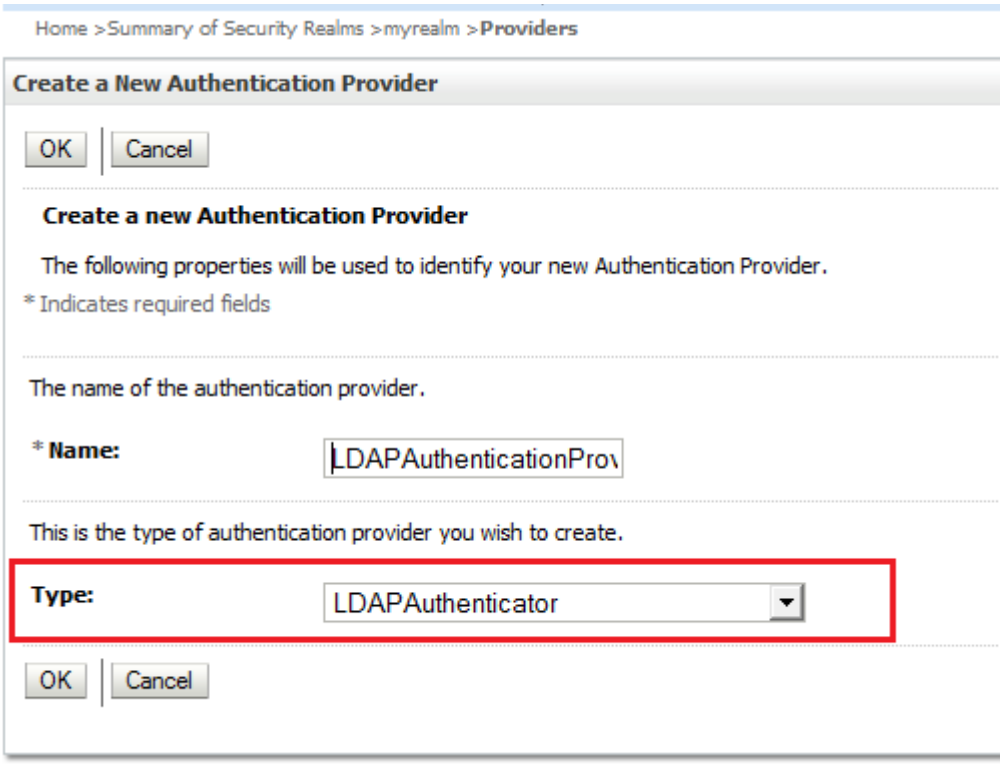
   We will configure Apache DS as

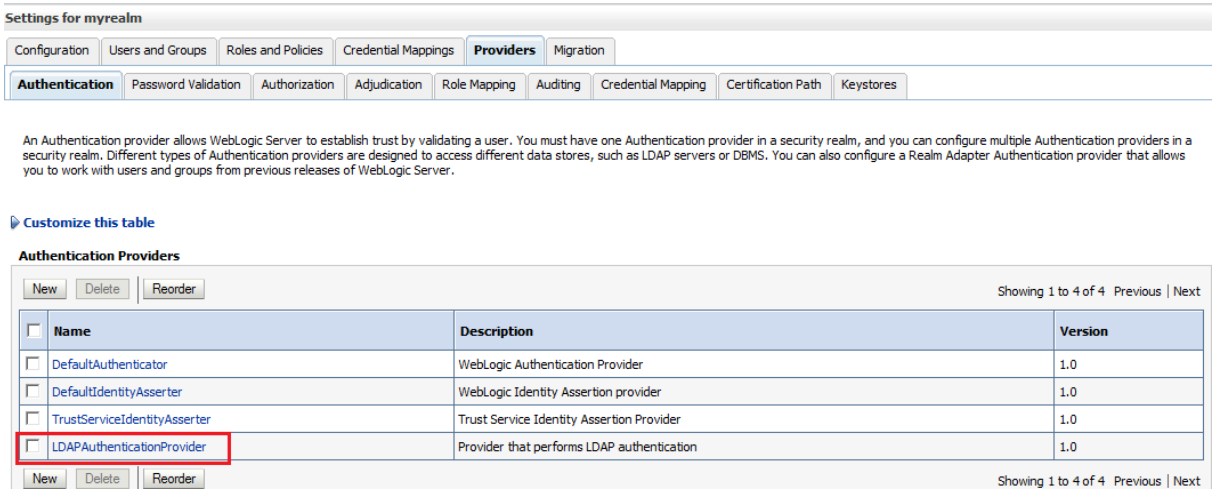
   - ***Identity Store for OPAM*** - an appropriate ***Authentication Provider*** will be configured in OPAM Weblogic Admin console (this will ***replace the Weblogic Embedded LDAP*** used in previous examples)
   - ***Managed Target within OIM*** - integrated via ICF LDAP Connector



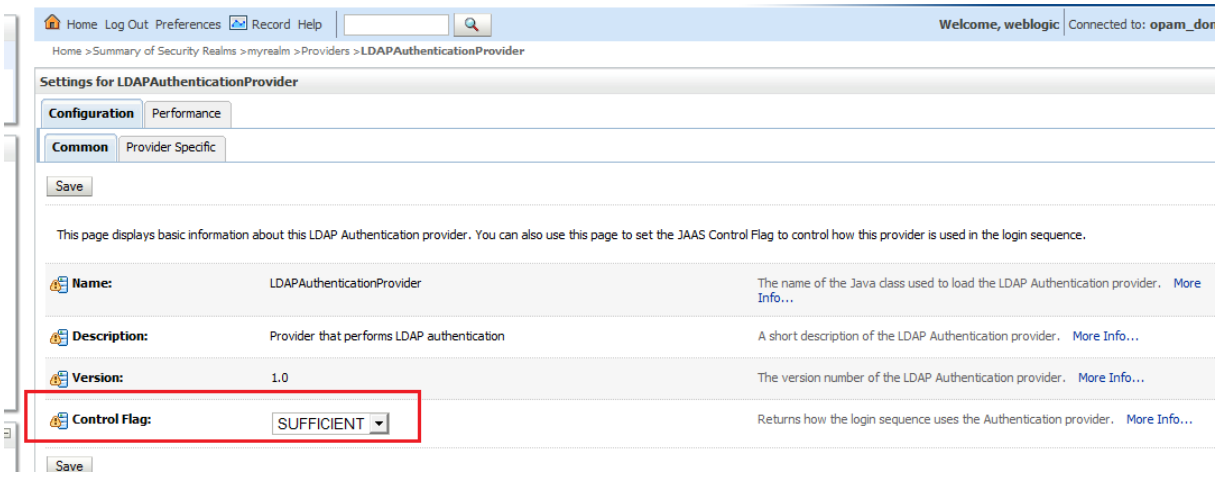


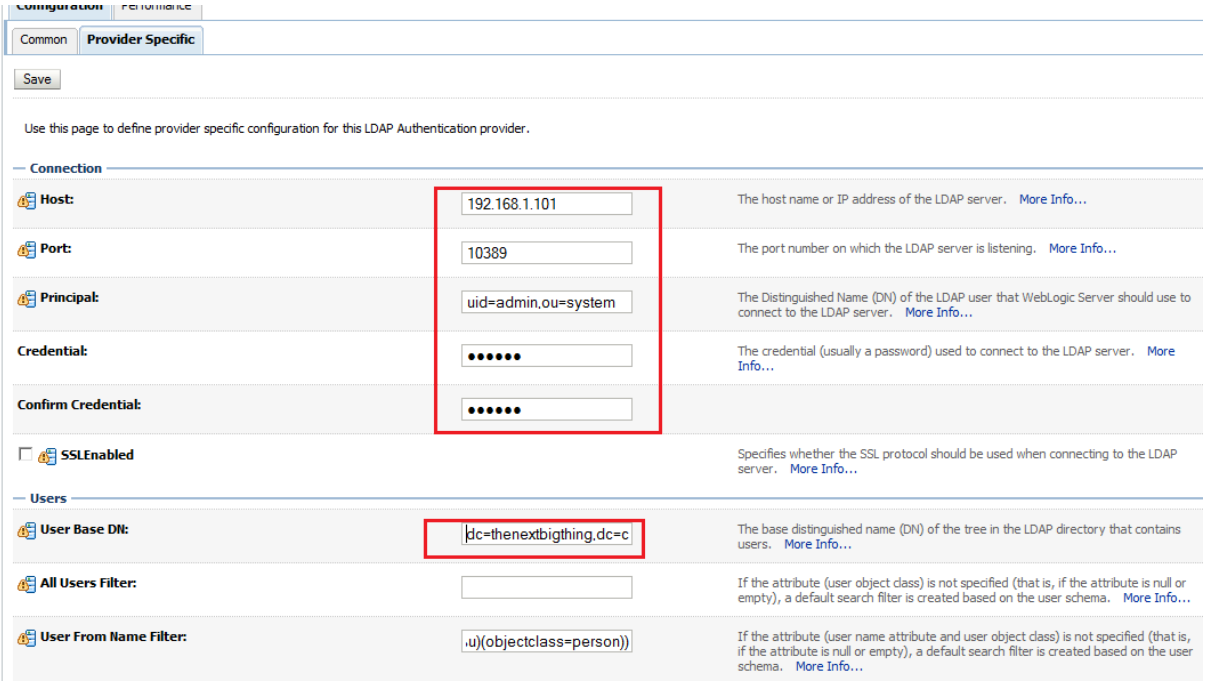
By Abhishek Gupta



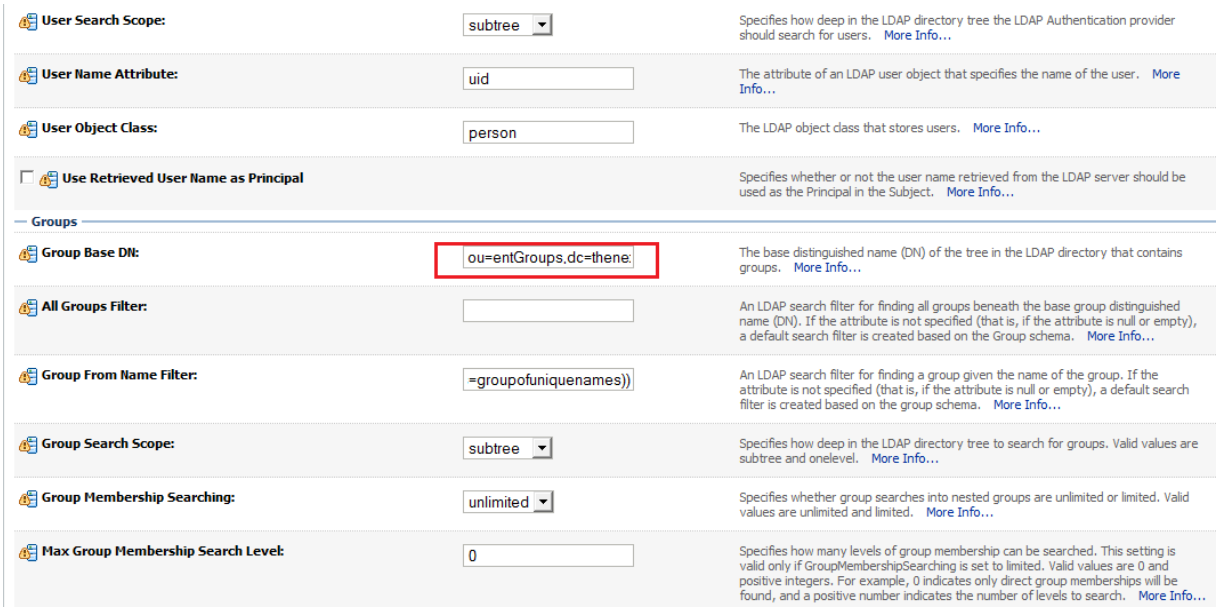


By Abhishek Gupta



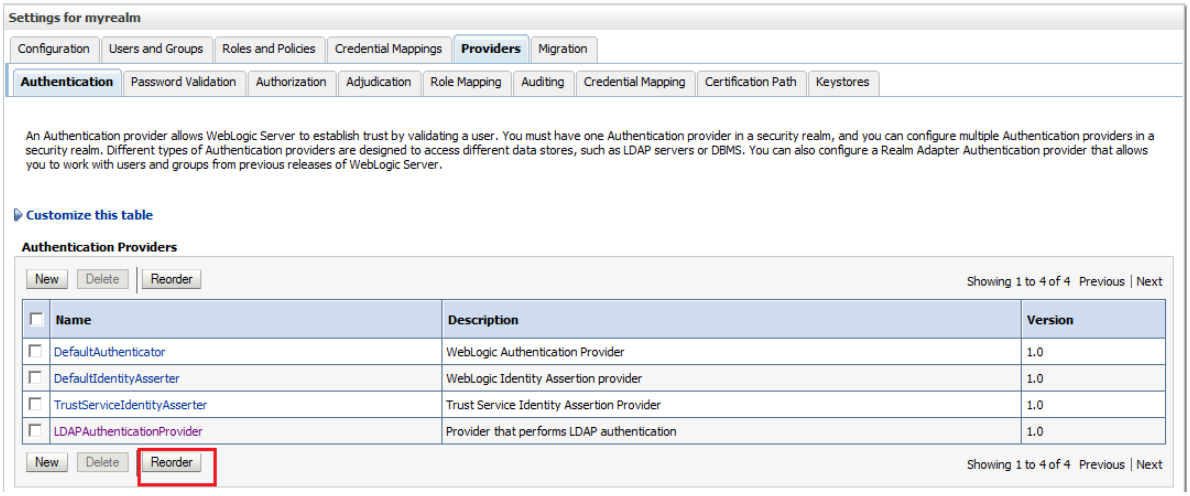


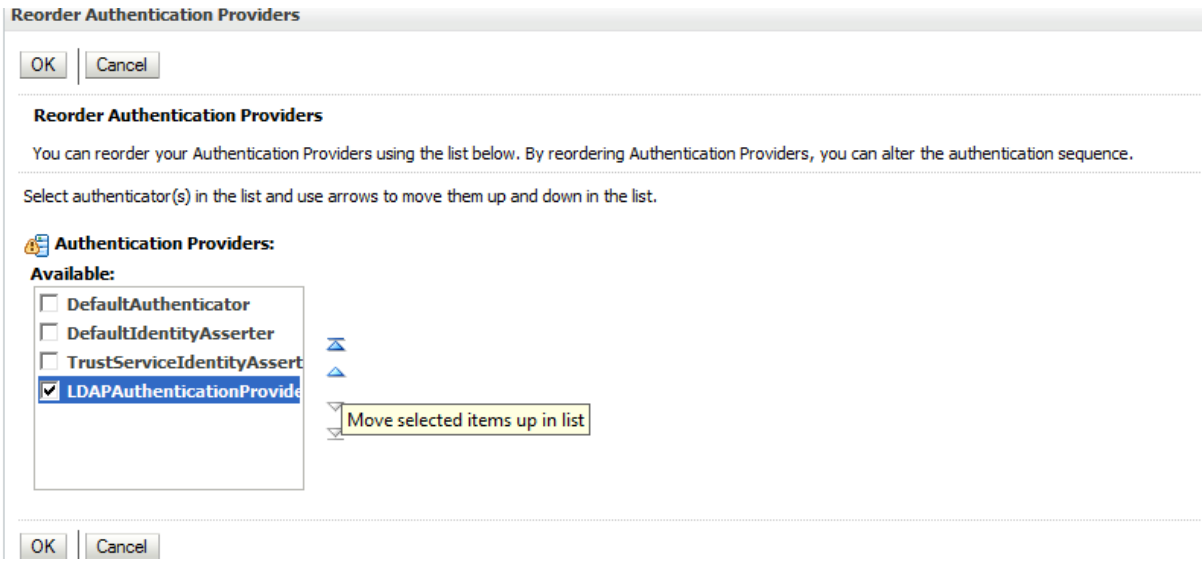
By Abhishek Gupta

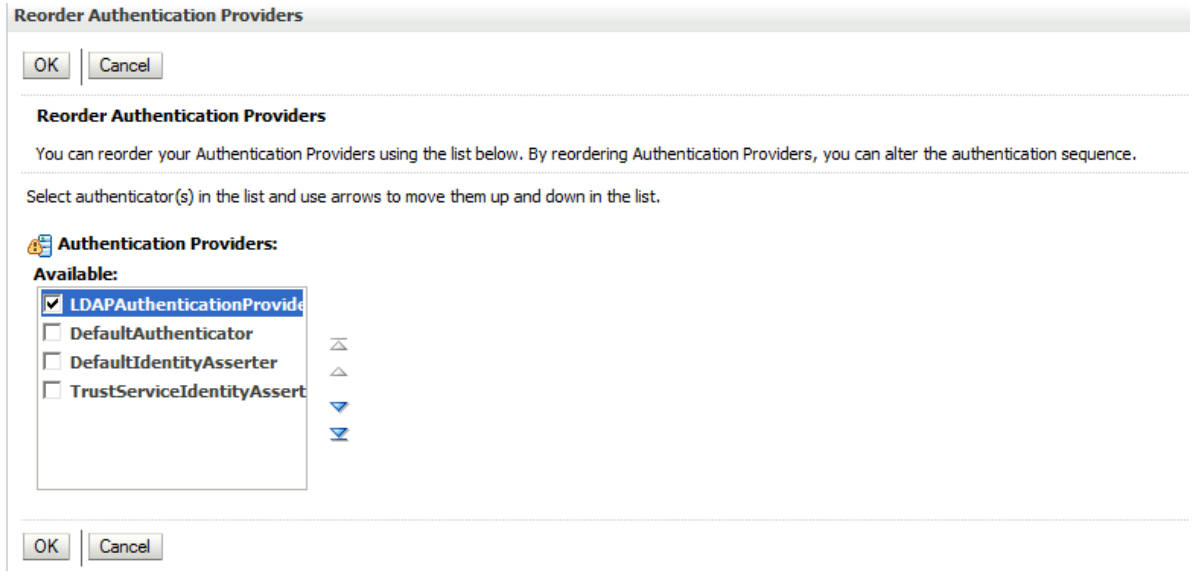


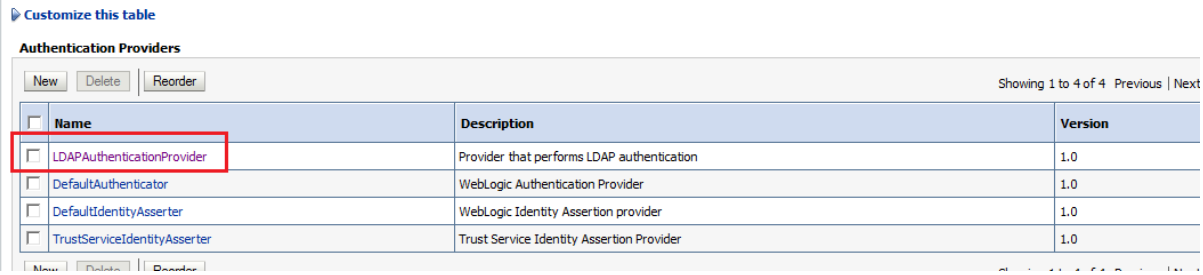
..... Leave all the other default values except for the ones which are highlighted

Reorder the provider



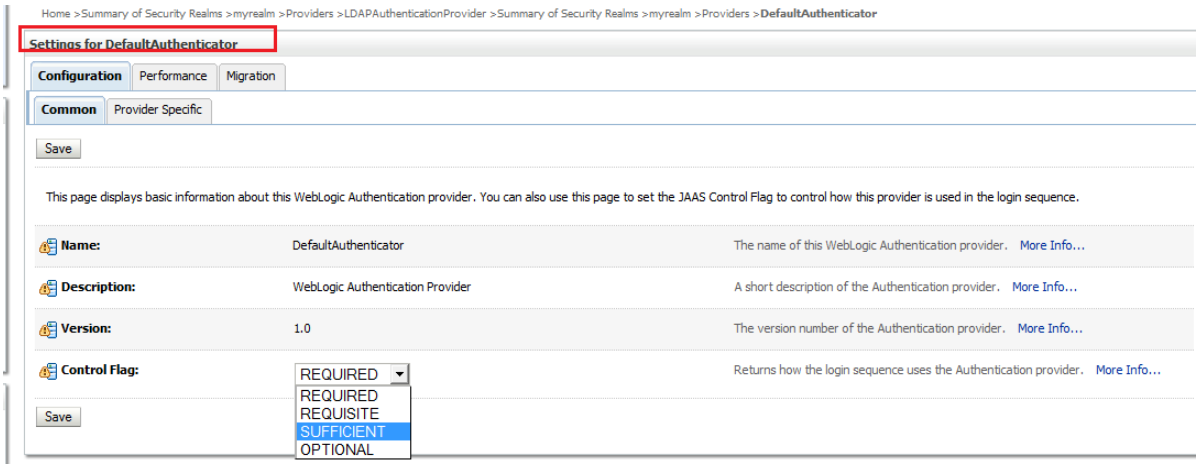


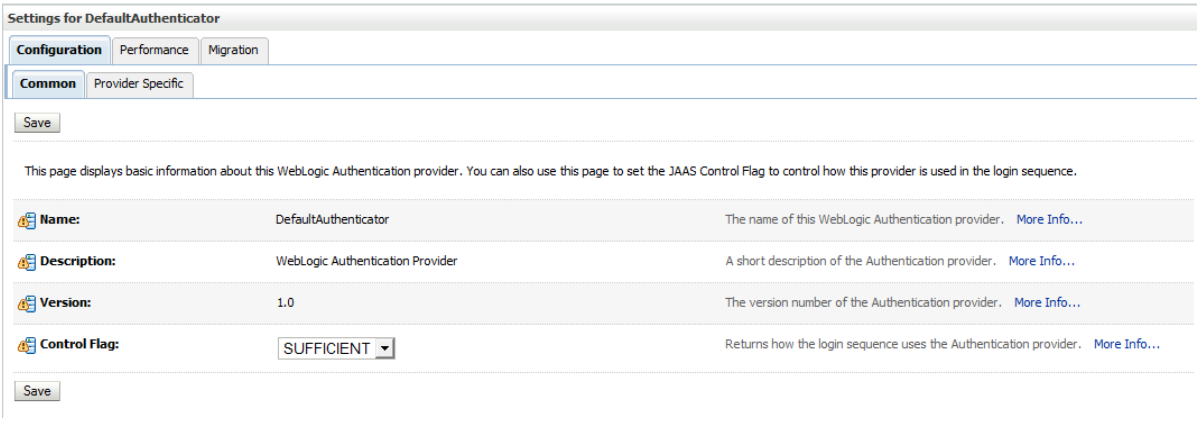




By Abhishek Gupta

Change Control Flag for Default Authenticator from REQUIRED to SUFFICIENT





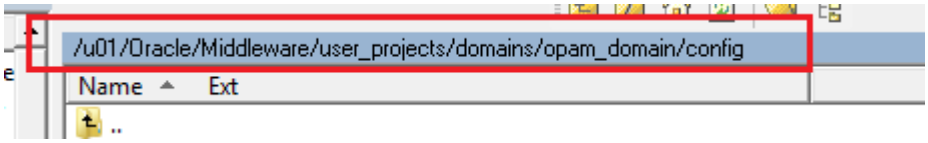
Restart Weblogic Admin and OPAM Managed Server

Note: On starting Weblogic Admin server, you might receive the below error

opam-weblogic-admi
n-server-error.txt

Do the following

Take a backup of your config.xml (OPAM_DOMAIN/config)



Change it as per below snapshot

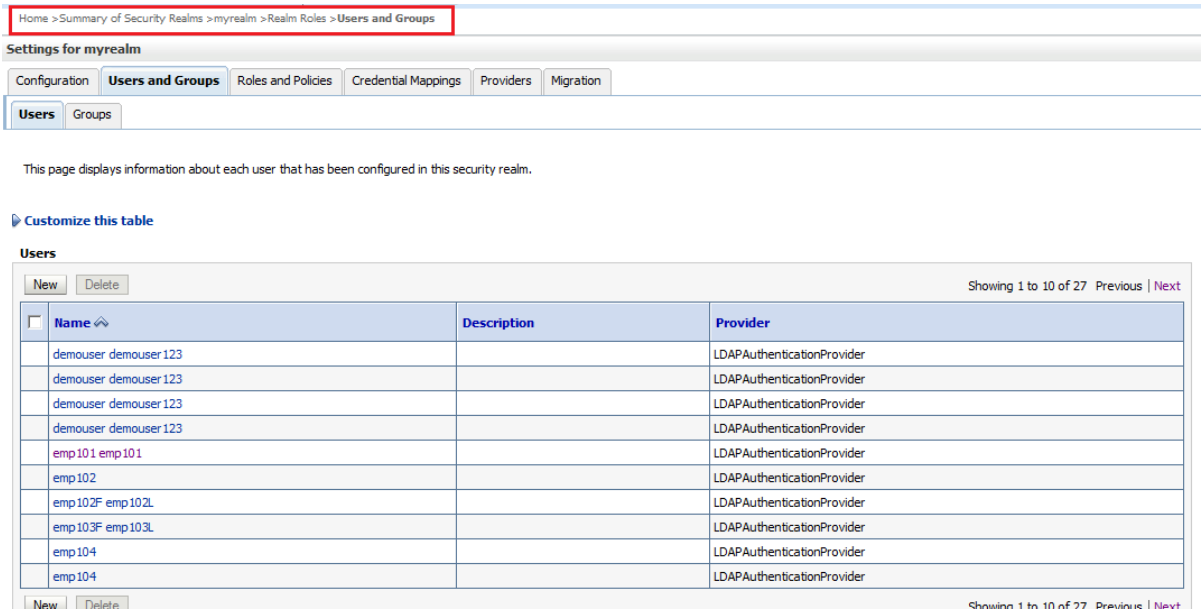
```
<domain-version>10.3.6.0</domain-version>
<security-configuration>
  <name>opam_domain</name>
  <realm>
    <sec:authentication-provider xsi:type="wls:open-ldap-authenticatorType">
      <sec:name>LDAPAuthenticationProvider</sec:name>
      <sec:control-flag>SUFFICIENT</sec:control-flag>
      <wls:host>192.168.1.101</wls:host>
      <wls:port>10389</wls:port>
      <wls:principal>uid=admin,ou=system</wls:principal>
      <wls:user-base-dn>ou=employees,dc=thenextbigthing,dc=com</wls:user-base-dn>
      <wls:credential-encrypted>{AES}VdpAgcG6HBJydIX2GVyfWq1KFcuS07efChV4w8NcwHI=</wls:credential-encrypted>
      <wls:group-base-dn>ou=entGroups,dc=thenextbigthing,dc=com</wls:group-base-dn>
```

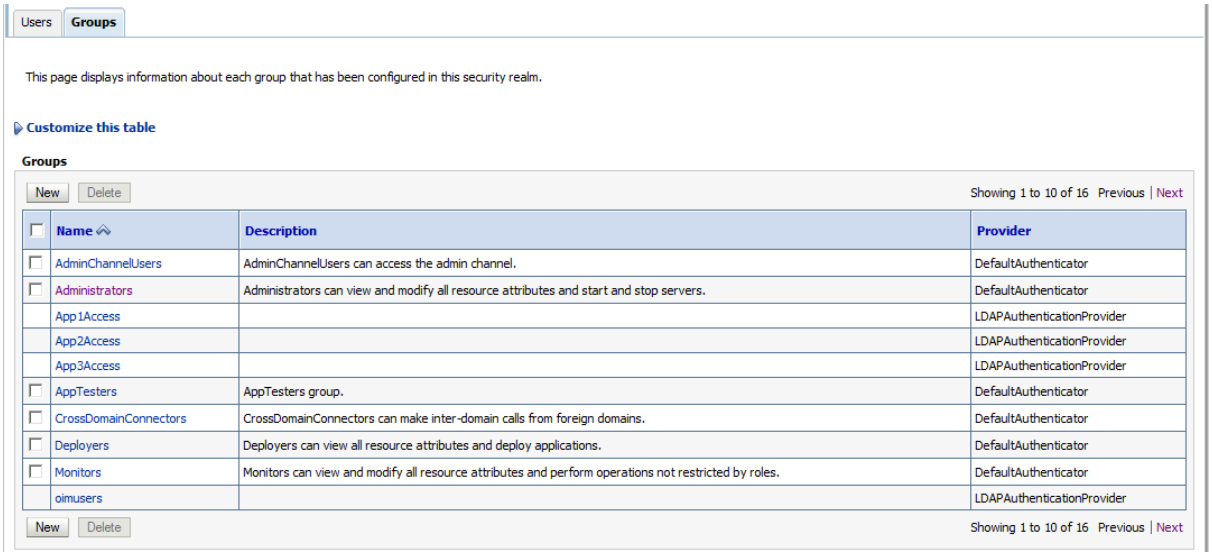
Start the Admin server again

Start the OPAM Managed Server after that

Sanity checks

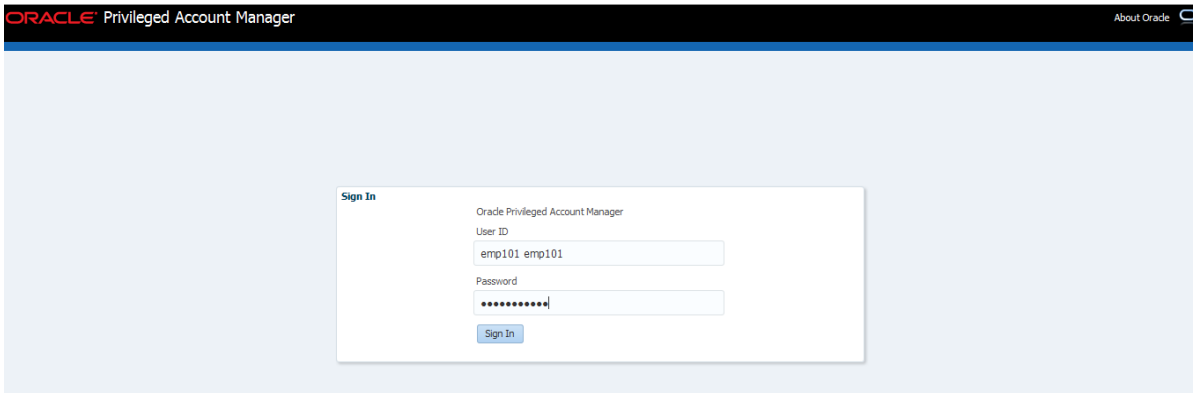
Check user and groups in Weblogic Admin Console

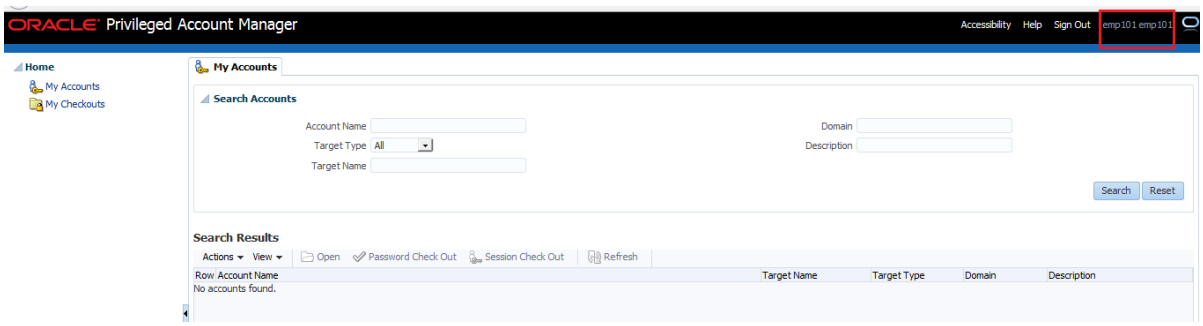




Log into OPAM using user credentials from LDAP (we'll use the user which is highlighted below)

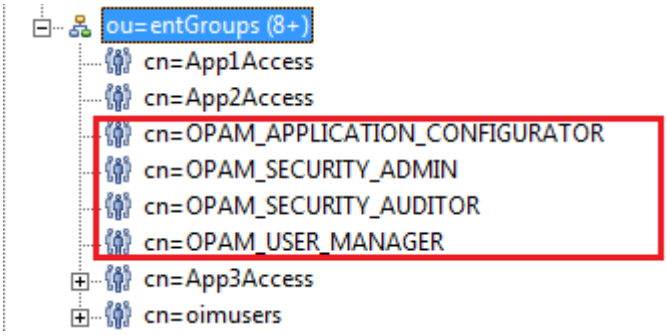
Name	Description	Provider
demouser demouser123		LDAPAuthenticationProvider
demouser demouser123		LDAPAuthenticationProvider
demouser demouser123		LDAPAuthenticationProvider
demouser demouser123		LDAPAuthenticationProvider
emp101 emp101		LDAPAuthenticationProvider
emp102		LDAPAuthenticationProvider
emp102F emp102L		LDAPAuthenticationProvider
emp103F emp103L		LDAPAuthenticationProvider
emp104		LDAPAuthenticationProvider
emp104		LDAPAuthenticationProvider





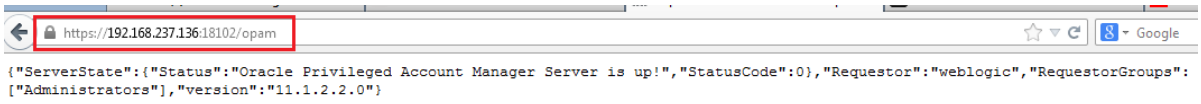
Create corresponding LDAP Roles in your Identity Store to map to the OPAM Admin Roles

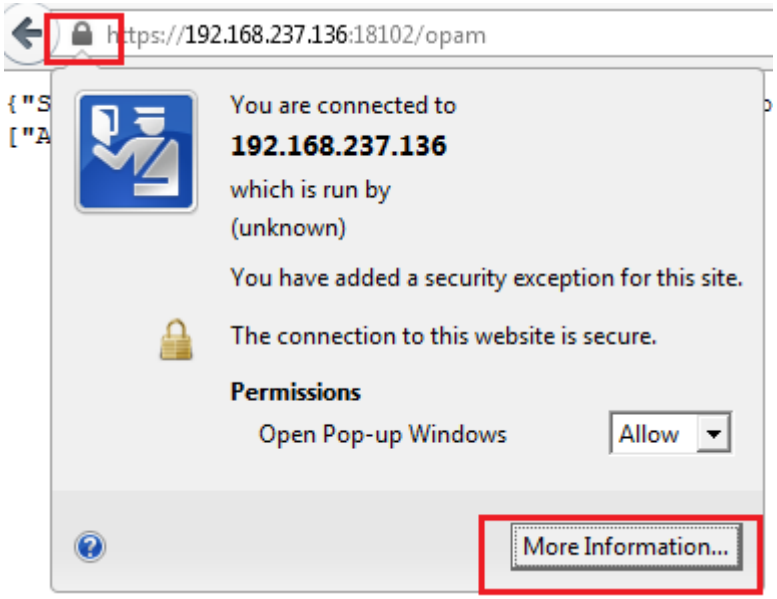
(Follow exact names as provided in http://docs.oracle.com/cd/E40329_01/admin.1112/e27152/und_security.htm#BGBFHEFC)

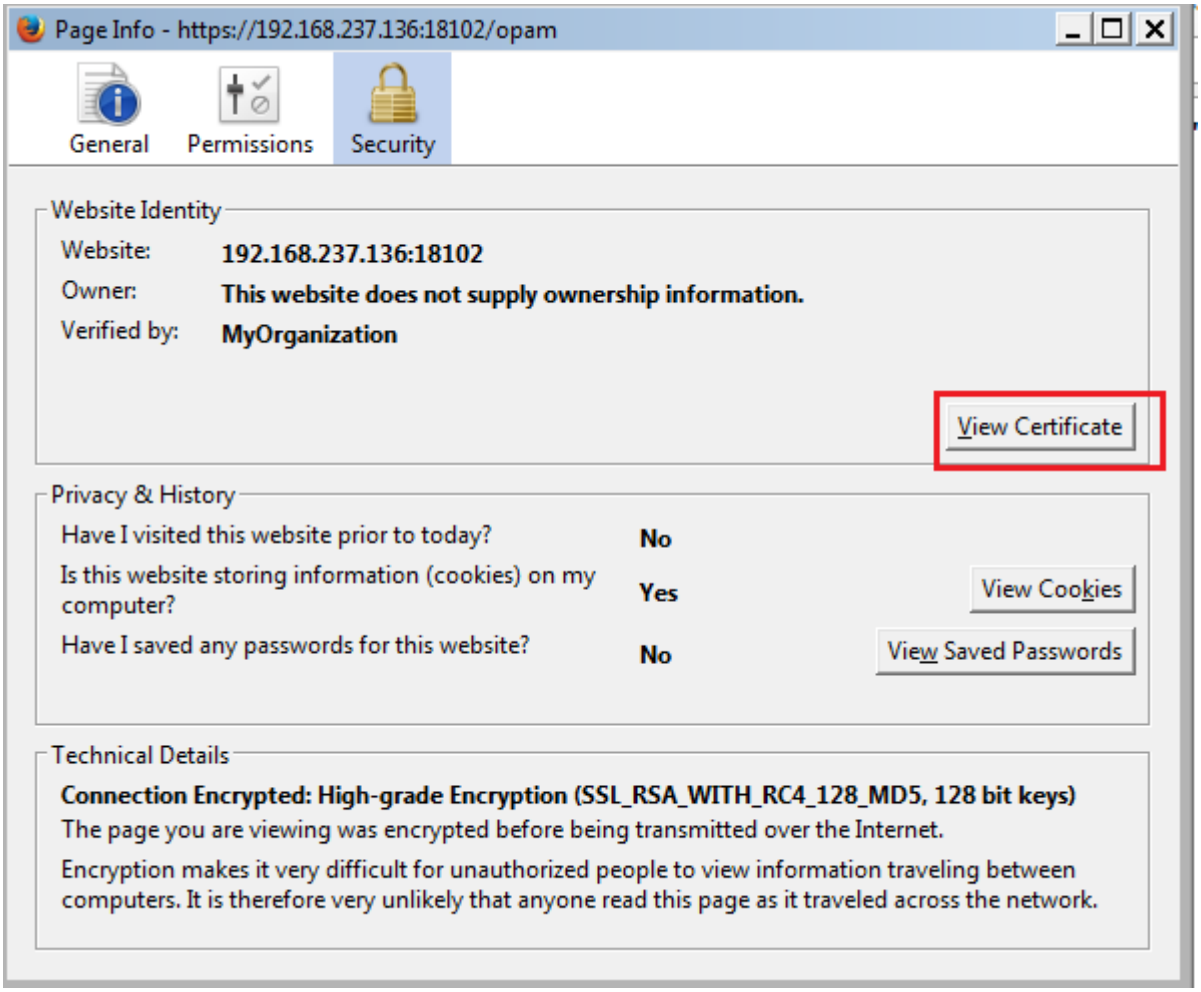


2. Add the OPAM CA certificate in OIM's Weblogic TrustStore in order for ***OIM to be able to call OPAM web services***

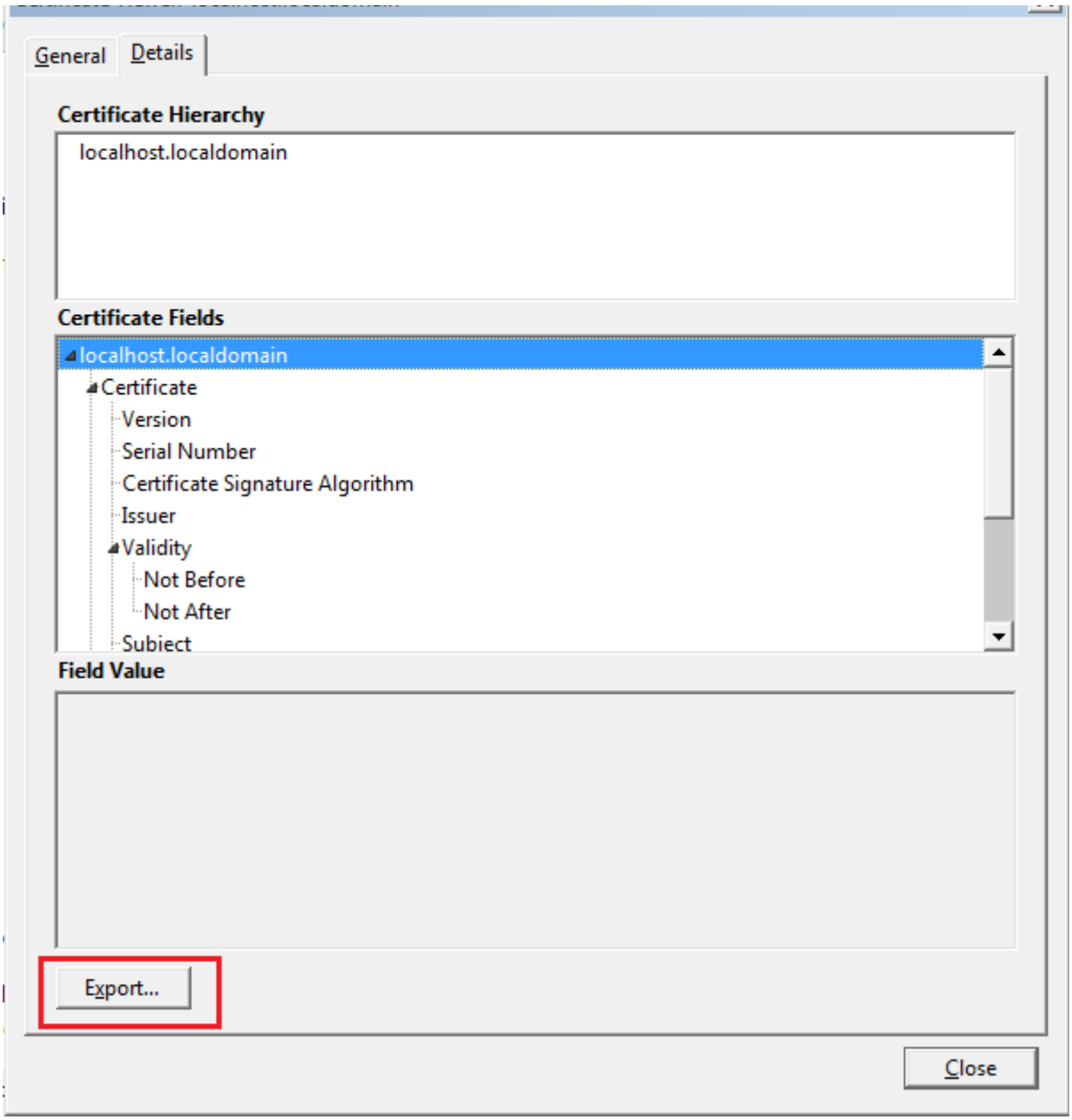
   Access OPAM Server







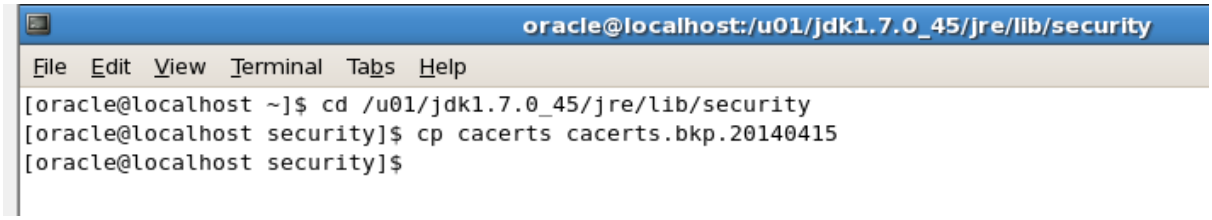
By Abhishek Gupta



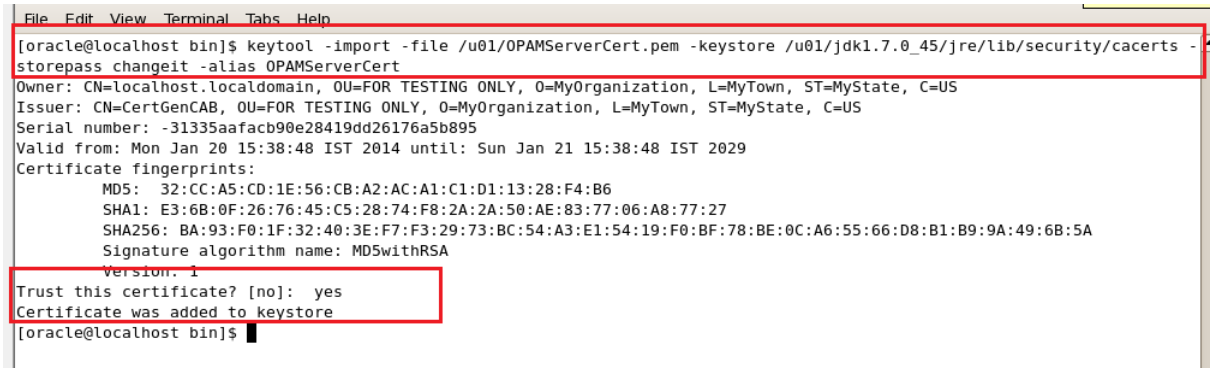
Save it on the OPAM machine

Import the same in to the JDK which your OPAM weblogic server

Note: Please take a backup if your original Truststore

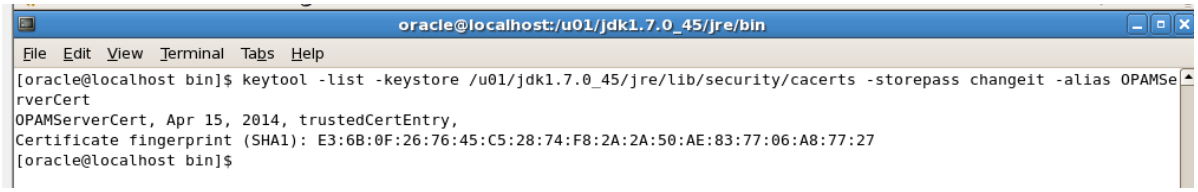


keytool -import -file /u01/OPAMServerCert.pem -keystore /u01/jdk1.7.0_45/jre/lib/security/cacerts -storepass changeit -alias OPAMServerCert



Confirm the same

keytool -list -keystore /u01/jdk1.7.0_45/jre/lib/security/cacerts -storepass changeit -alias OPAMServerCert



3. Create an OPAM Admin account

Create a user in LDAP (Apache) who you want to assign as the OPAM ADmin

DN: uid=apacheopamadmin,ou=employees,dc=thenextbigthing,dc=com

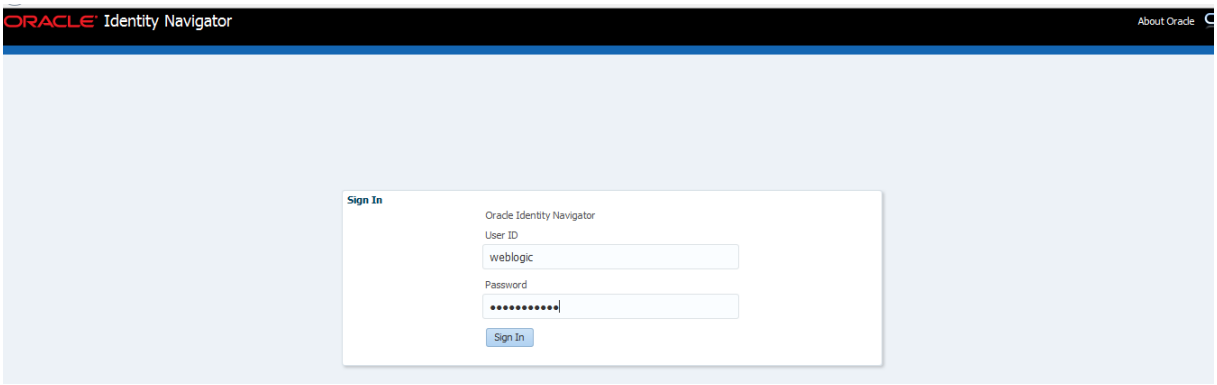
Attribute Description	Value
objectClass	***inetOrgPerson (structural)***
objectClass	***organizationalPerson (structural)***
objectClass	***person (structural)***
objectClass	***top (abstract)***
cn	**apacheopamadmin**
sn	**opamadmin**
givenname	DEMOUSERF_U
mail	apacheopamadmin@testmail.com
uid	apacheopamadmin
userPassword	SSHA hashed password

Users

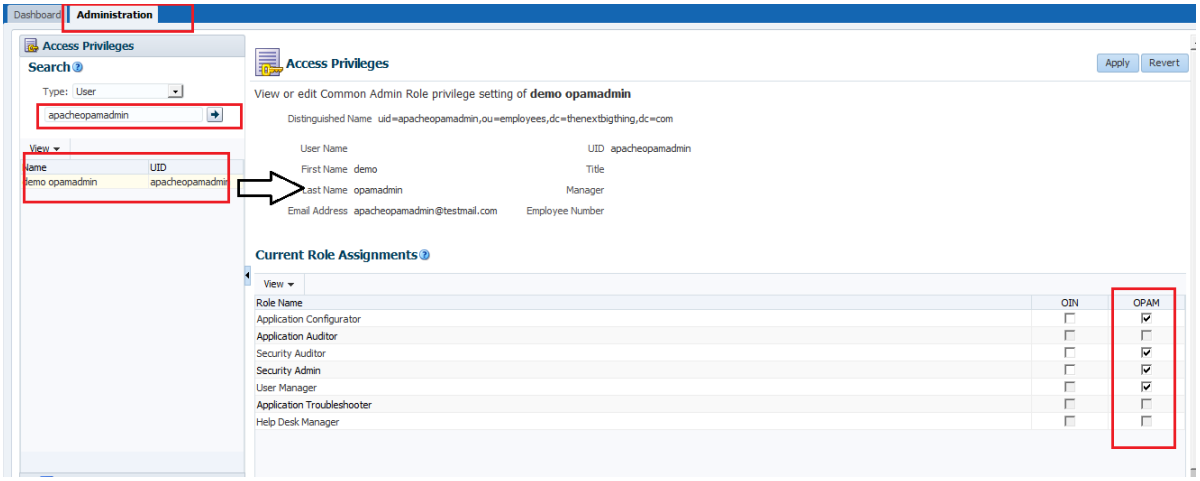
New Delete

Name	Description	Provider
apacheopamadmin		LDAPAuthenticationProvider
demouser demouser123		LDAPAuthenticationProvider
demouser demouser123		LDAPAuthenticationProvider
demouser demouser123		LDAPAuthenticationProvider
demouser demouser123		LDAPAuthenticationProvider
emp101 emp101		LDAPAuthenticationProvider
emp102		LDAPAuthenticationProvider
emp102F emp102L		LDAPAuthenticationProvider
emp103F emp103L		LDAPAuthenticationProvider
emp104		LDAPAuthenticationProvider

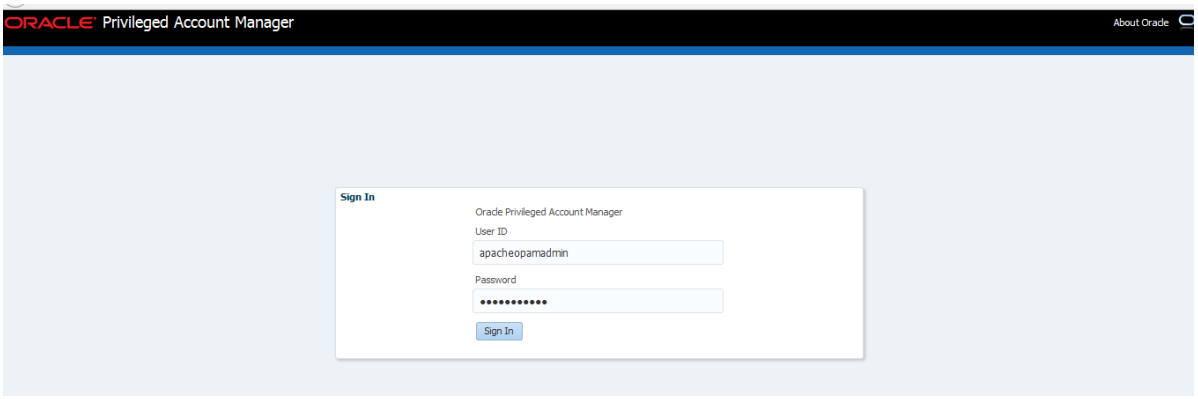
Log into the OINAV console to assign OPAM specific Admin Roles



Provide all the OPAM Admin Roles

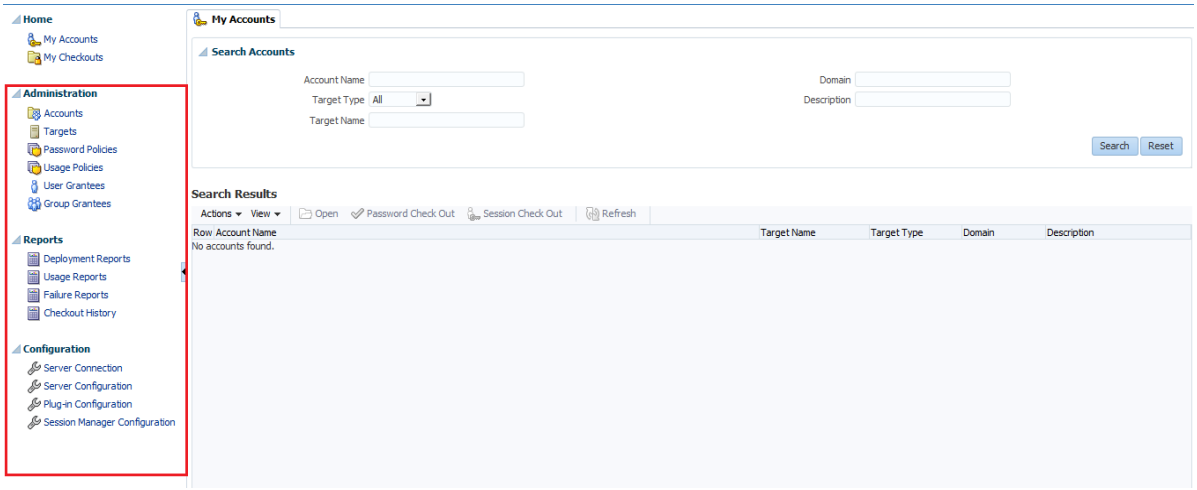


Log into OPAM with the user to confirm



He has all the authorization as per Admin Roles

By Abhishek Gupta



4. Run ***opamSetup*** script

export APP_SERVER=weblogic

export OIM_ORACLE_HOME=/u01/Oracle/Middleware/Oracle_IDM1

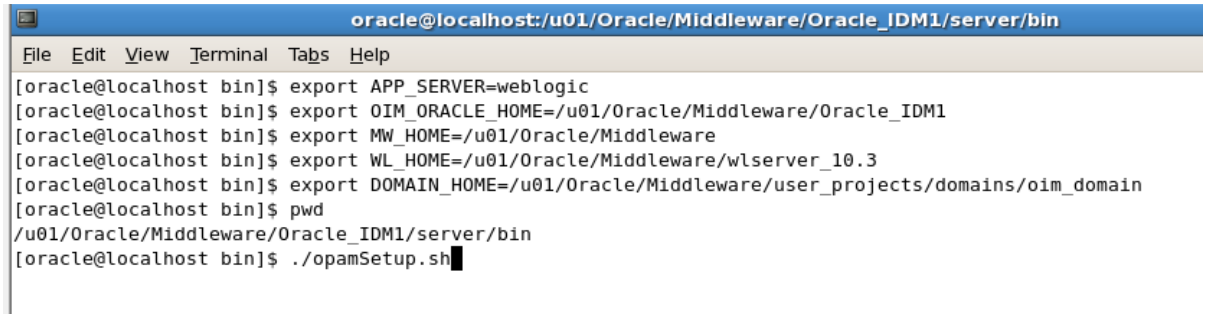
export MW_HOME=/u01/Oracle/Middleware

export WL_HOME=/u01/Oracle/Middleware/wlserver_10.3

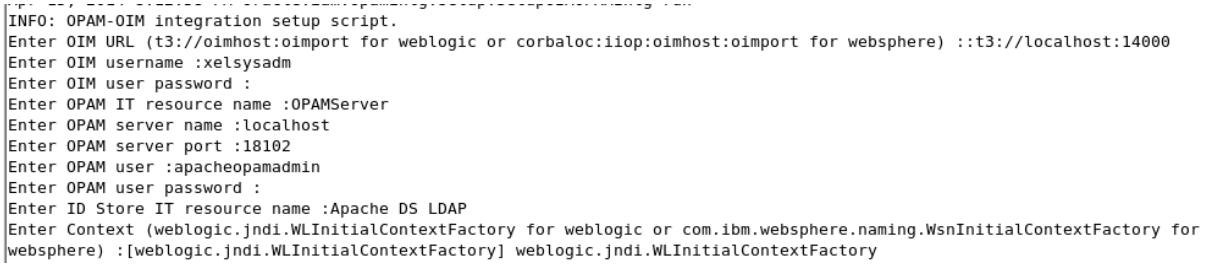
export DOMAIN_HOME=/u01/Oracle/Middleware/user_projects/domains/oim_domain

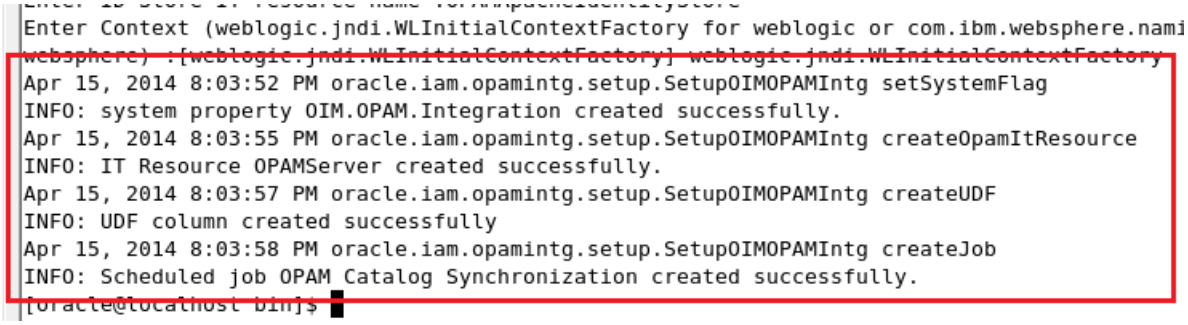
cd /u01/Oracle/Middleware/Oracle_IDM1/server/bin

./opamSetup.sh



Start entering details as prompted

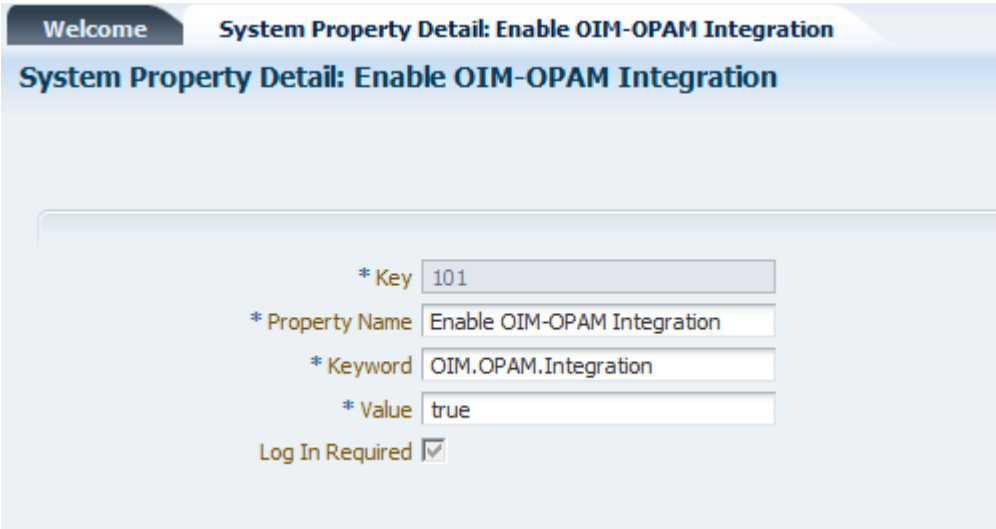




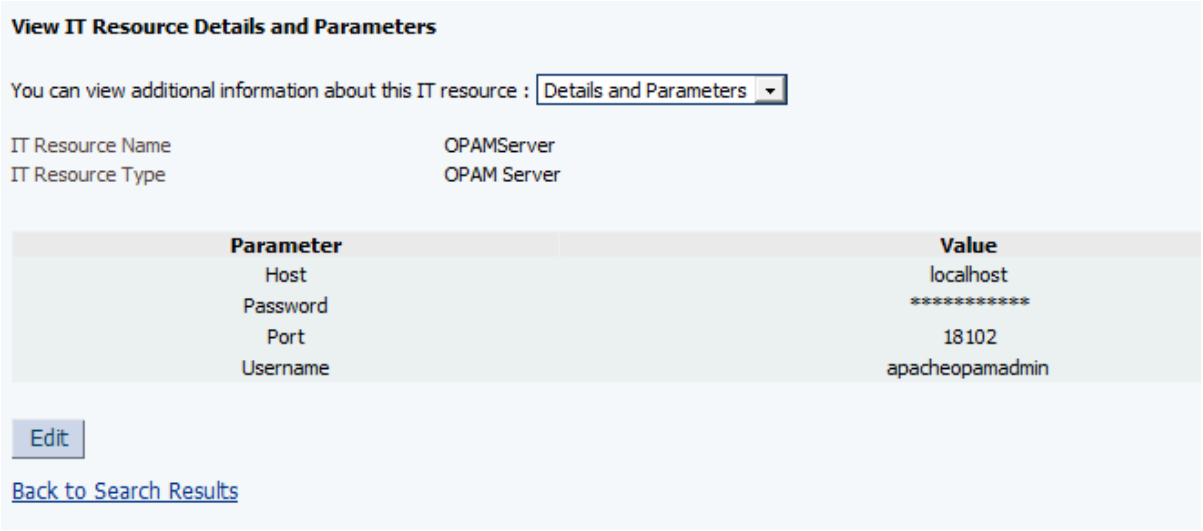
Confirm the artifacts on OIM end

Log into OIM

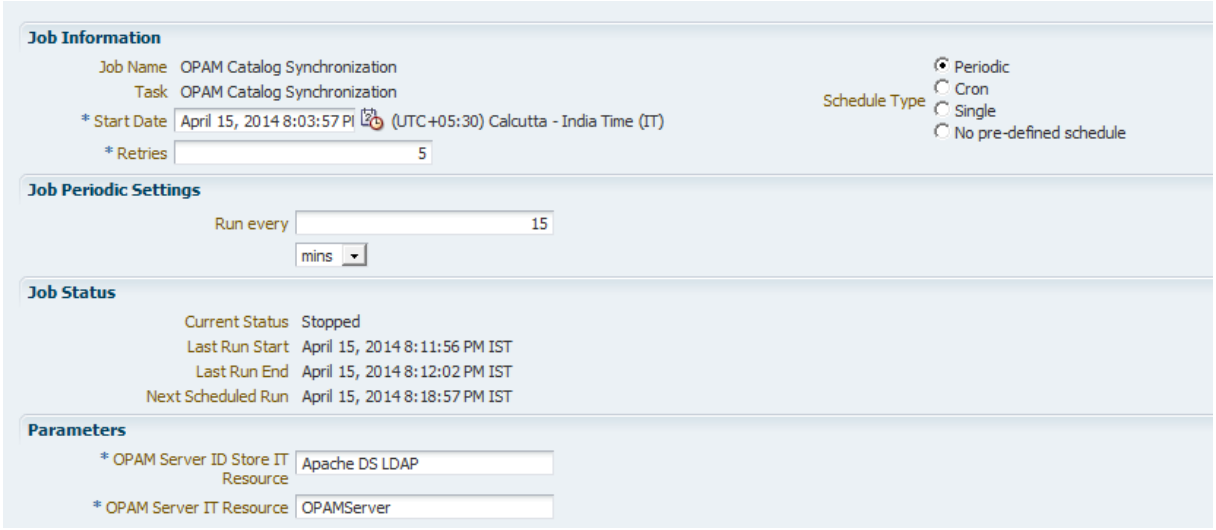
Check System Property



Check IT Resource

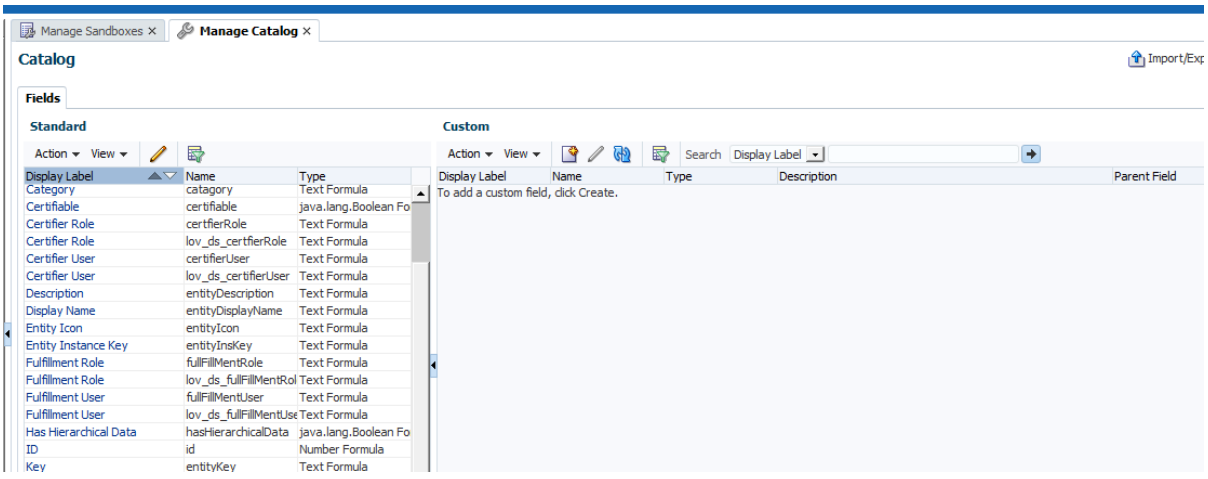


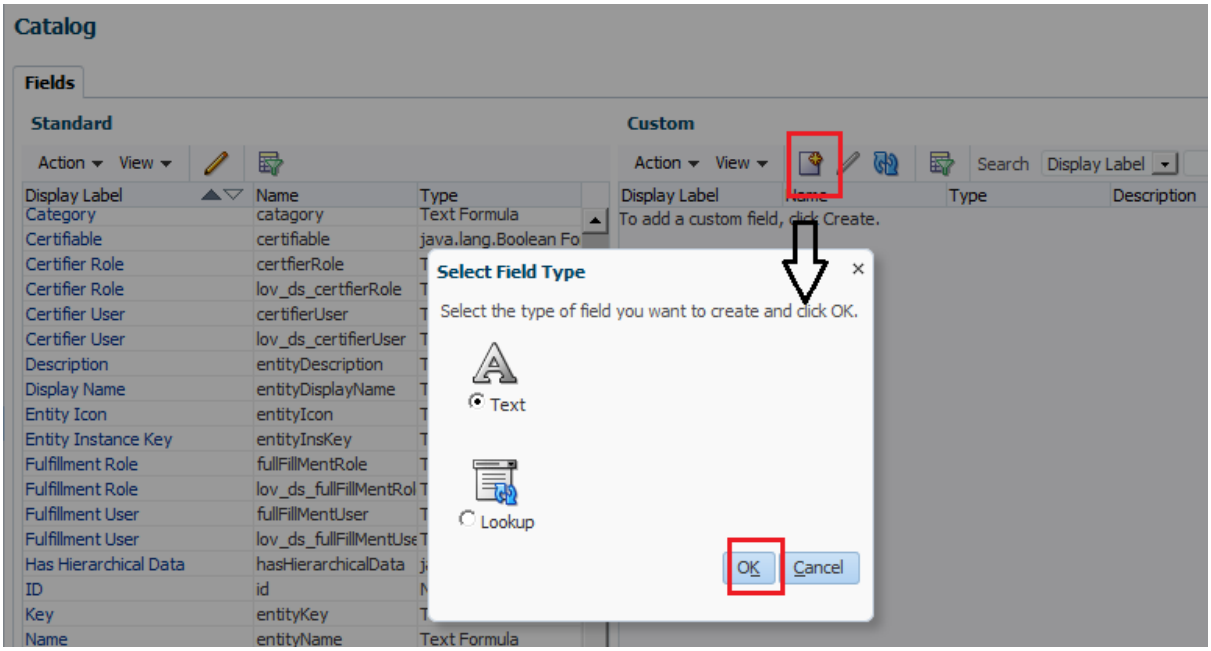
Check Schedule Job



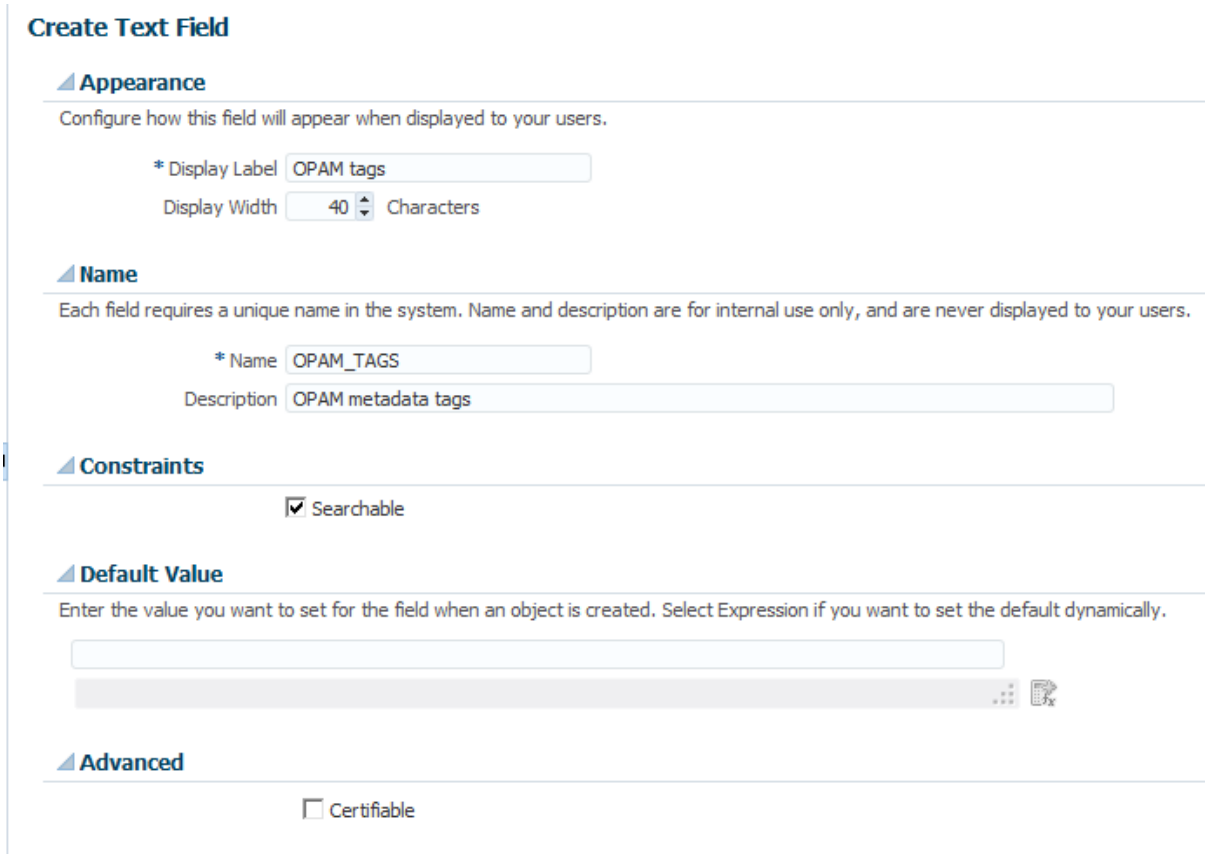
5. Create OPAM_TAGS - this is a UDF in the Catalog form

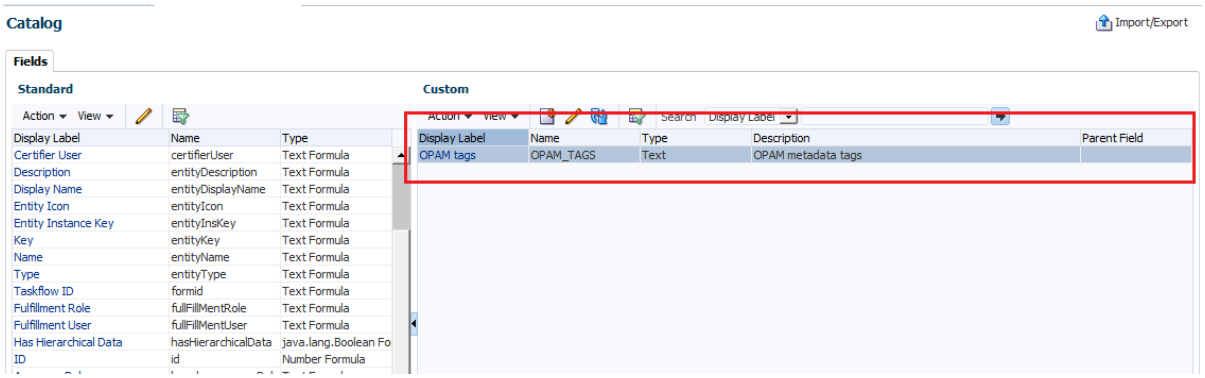
Create a sandbox and edit the Catalog Form in OIM





By Abhishek Gupta



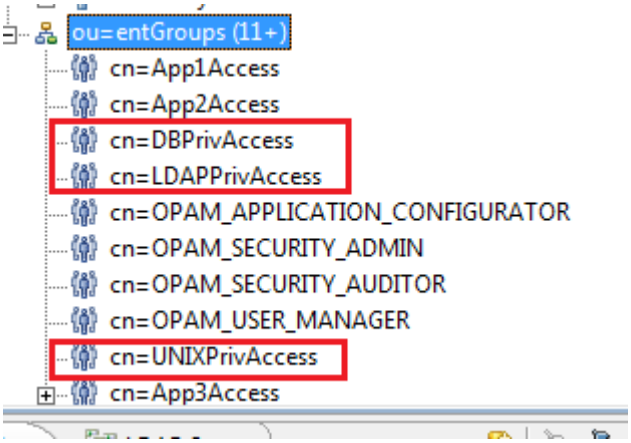


Publish the Sandbox

6. Create groups in your LDAP server

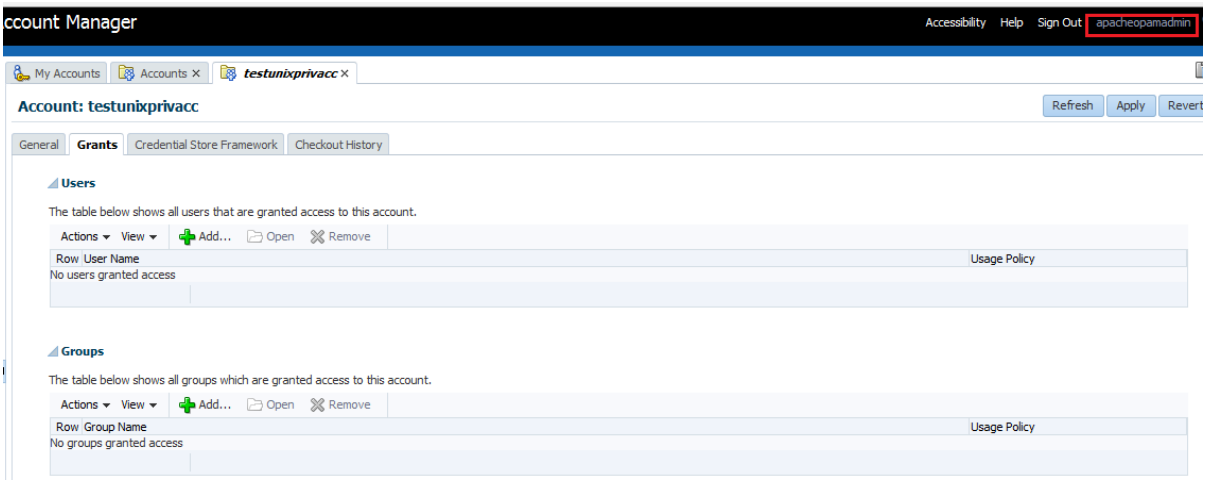
These groups would be configure in OPAM to manage access to privileged accounts and targets

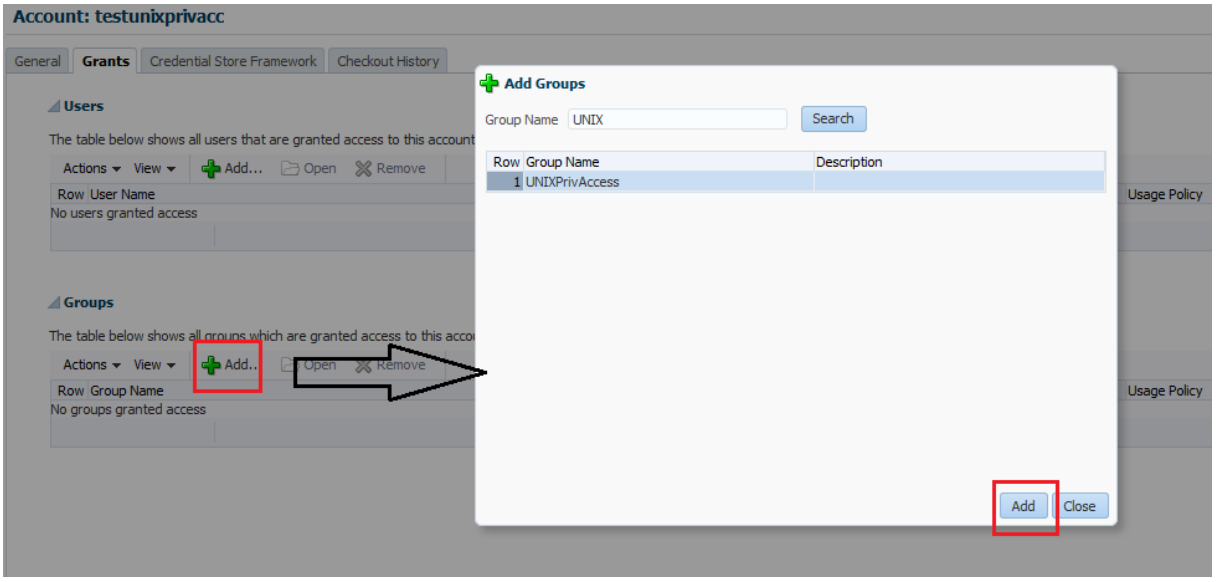
Groups for LDAP, DB and UNI privilege accounts



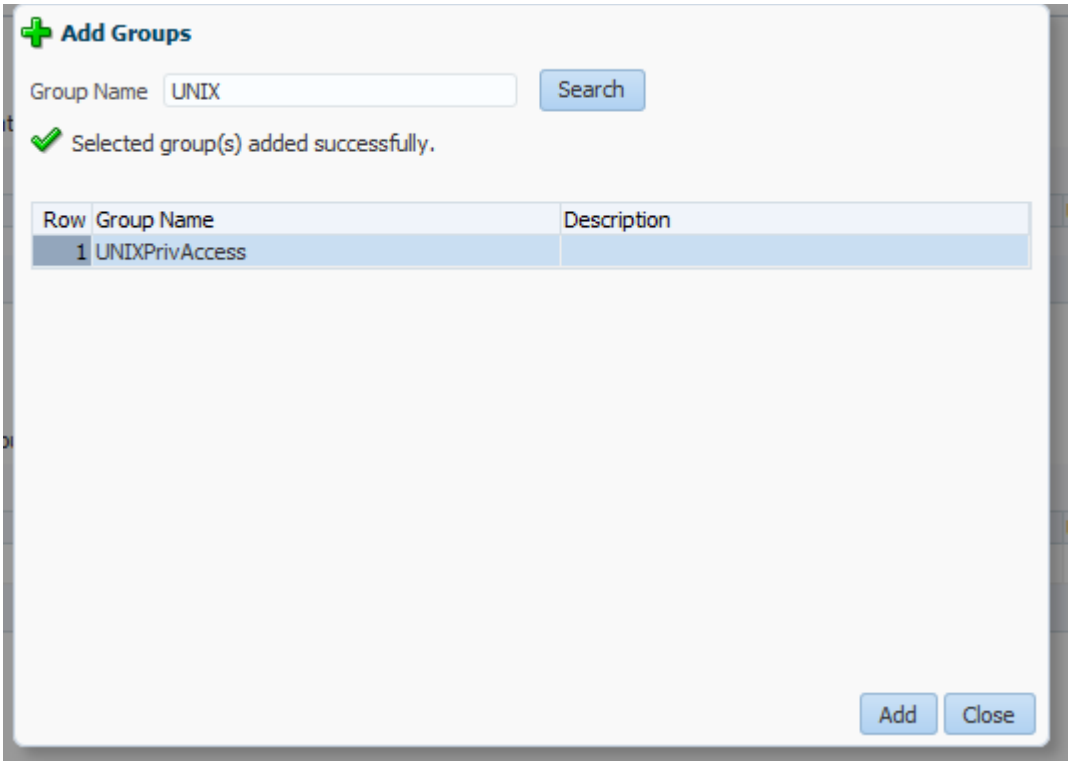
7. Assign Grants to the privilege accounts based on groups

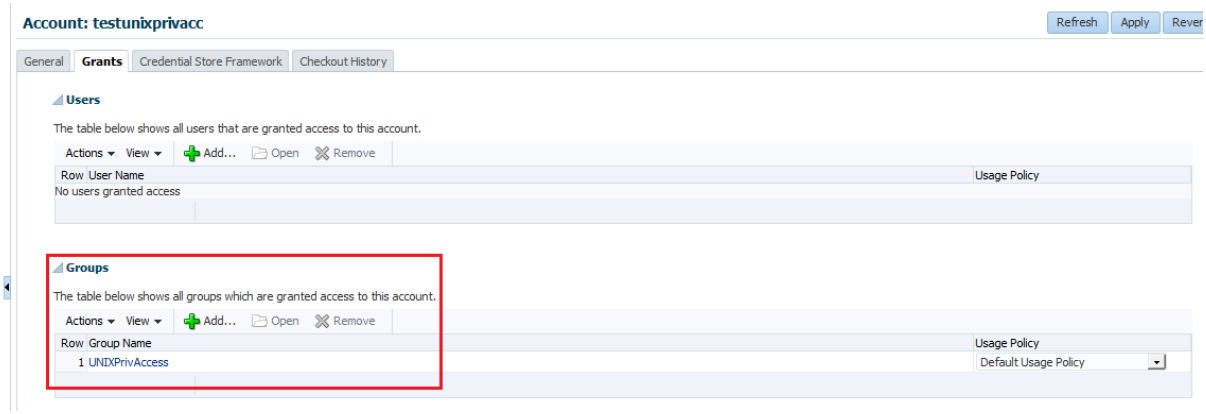
Log into OPAM as admin



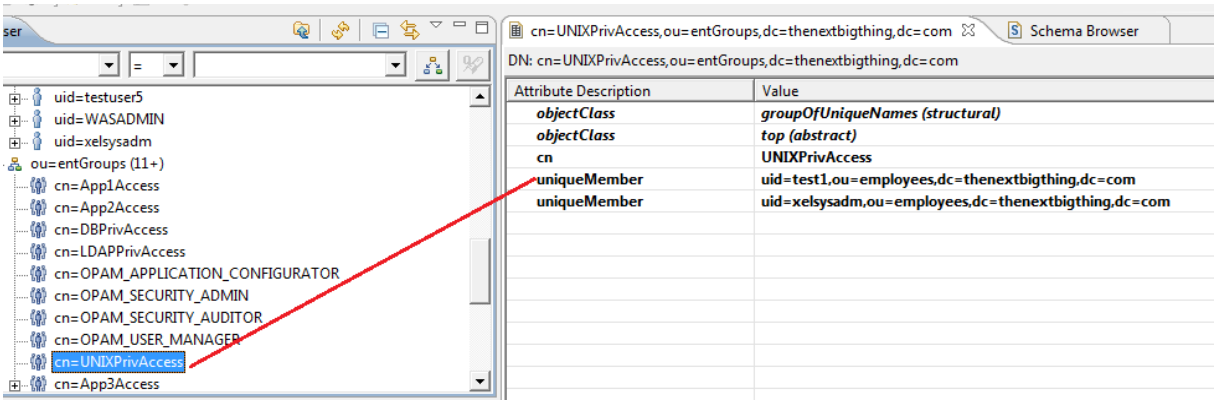


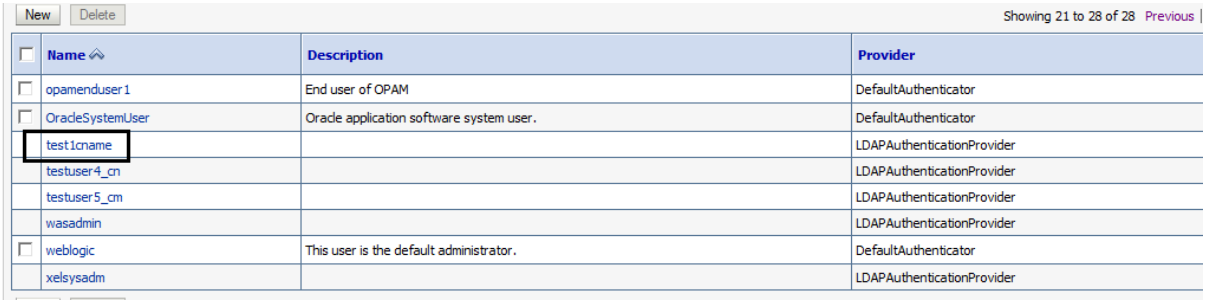
By Abhishek Gupta



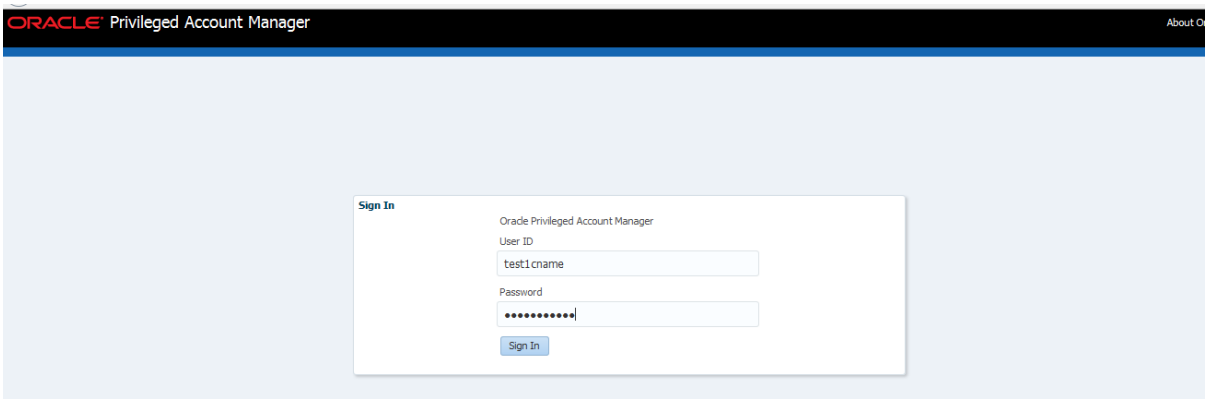


8. Log into OPAM as an end user who is a member of the Group configured above and see if he able to check out the UNIX account

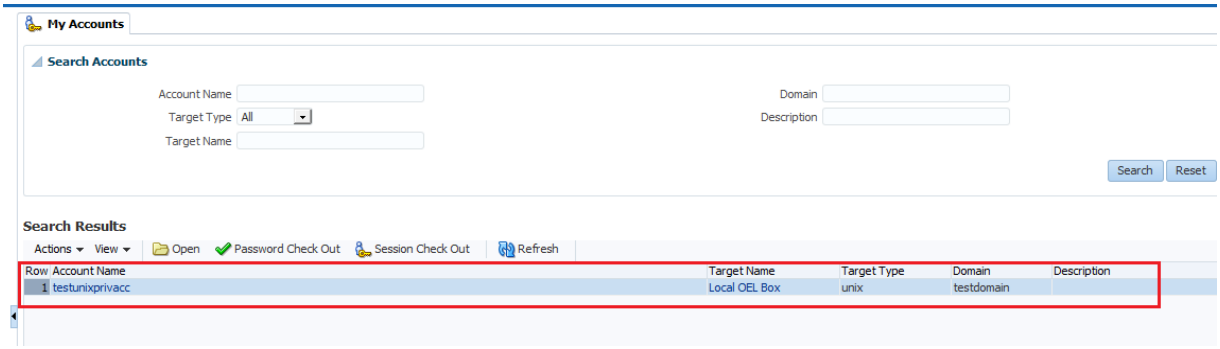


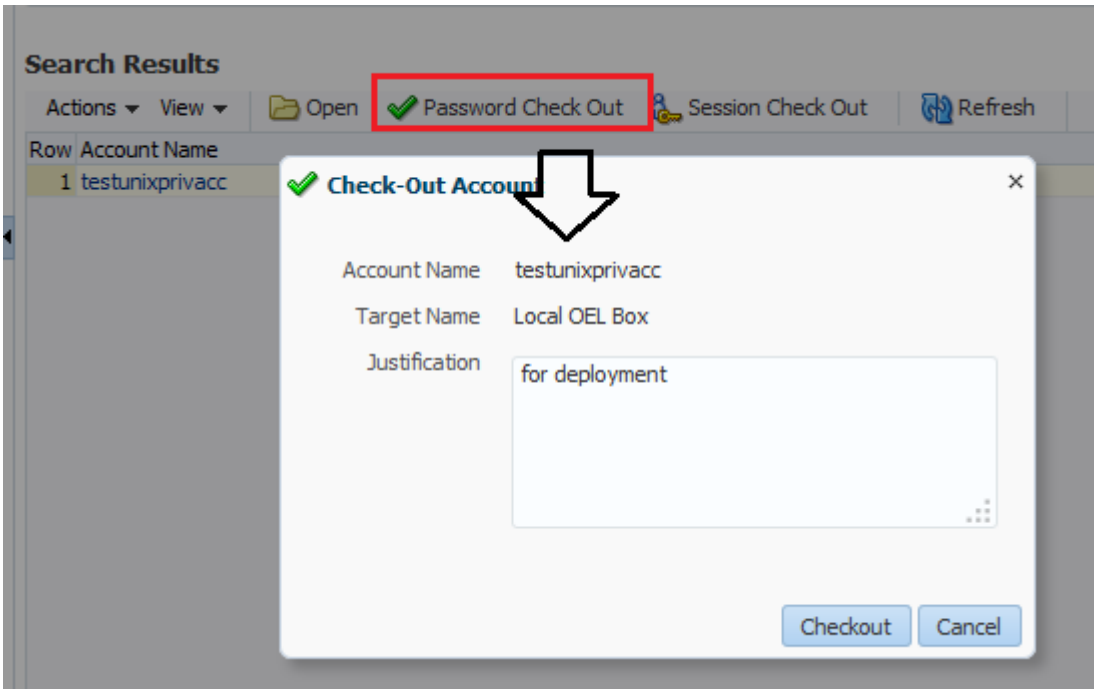


We'll use the above user since he is a member if the UNIXAccess group in LDAP



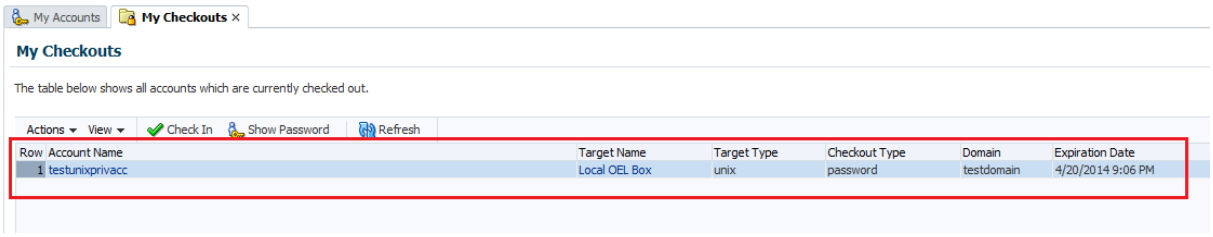
He has access to UNIX privileged account



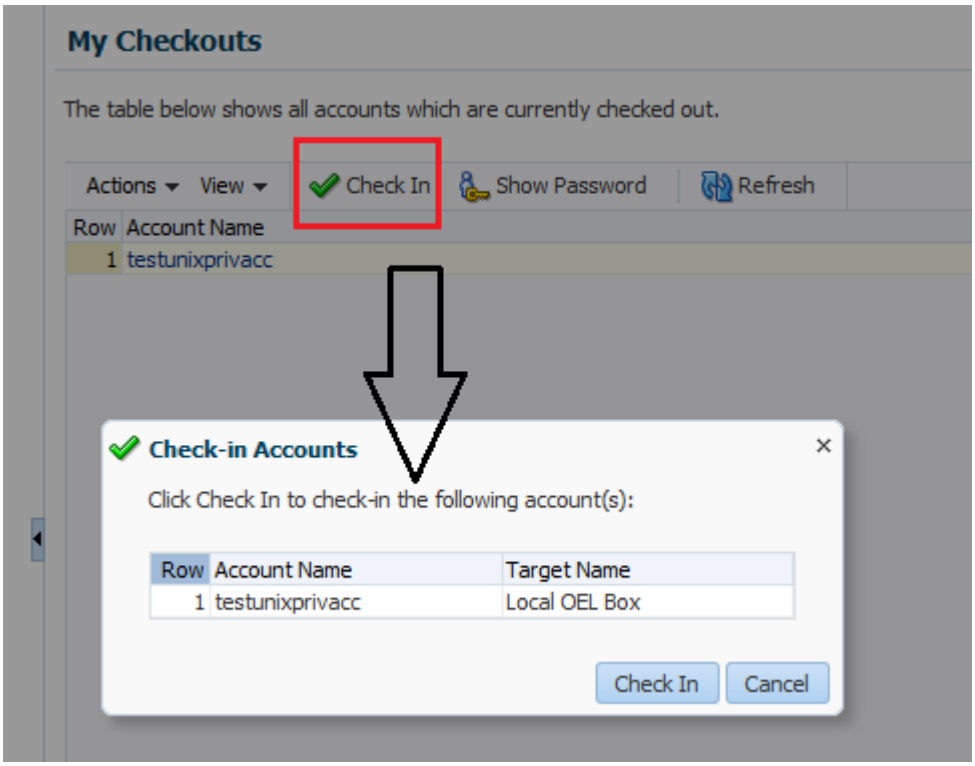


Let's confirm if it's checked out

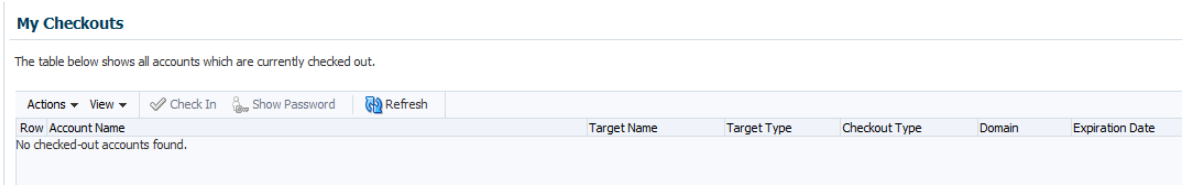
By Abhishek Gupta



We can safely check it in back again



Checked back in



By Abhishek Gupta

The same process is applicable for any Target/account - DB, LDAP etc